Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A user authentication system, comprising:

a registration station provided with an information acquisition device for obtaining biological individuality data for distinguishing individuality of a user[[,]];

an authentication card issuing station that issues to the user a user authentication card recorded with a divided part of the biological individuality data[[,]];

an authentication access terminal provided with an authentication-card reader for reading the information of the user authentication card and an identity acquisition device for inputting biological individuality data of the user[[,]]; and

at least one certification authority that is connected to the authentication access terminal through an information communication channel,

wherein the certification authority holds the record of the remaining part of the biological individuality data that have obtained at the registration station but not recorded in the user authentication card, the recorded contents in the user authentication card read out by the authentication card reader are compared with the biological individuality data of the user obtained on the spot through the identity acquisition device to authenticate identification of the user at the authentication access terminal, and

if a higher level of authentication is required, the certification authority compares the biological individuality data of the user obtained at the authentication access terminal with the part of the biological individuality data missing in the user authentication card in response to inquiry from the authentication access terminal and sends the comparison result to the authentication access terminal for further authentication[[.]],

wherein the two or more certification authorities dividedly record the remaining part of the biological individuality data obtained at the registration station but not recorded in the user authentication card, and one certification authority compares the biological individuality data of the user input at the authentication access terminal with the part of the biological individuality data stored in the certification authority in response to inquiry from the authentication access terminal or other certification authority for further authentication.

2. (Currently Amended) [[A]] The user authentication system according to claim 1, wherein the user authentication card has [[an]] a computing function and the computing function executes a calculation of authenticating ~~personal identification~~ said user authentication card at the authentication access terminal.

3. (Currently Amended) [[A]] The user authentication system according to claim [[2]] 1, wherein [[the]] information exchanged through the information communication channel is encrypted.

4. (Cancelled)

B1

5. (Currently Amended) [[A]] The user authentication system according to ~~any of~~ ~~claims~~ claim 1, wherein the certification authority is provided with a memory device for recording the biological individuality data obtained at the registration station.

6. (Currently Amended) [[A]] The user authentication system according to ~~any of~~ ~~claims~~ claim 1, wherein ~~plural~~ a plurality of different kinds of biological individuality data are registered so that different transactions ~~can be conducted~~ of different kinds of biological individuality data can be accessed and compared in response to ~~the kind of the~~ different input data.

7-19. (Cancelled)

20. (New) A system, comprising:

an authentication card including a first portion of a first biological individuality data, wherein said first biological individual data is divided into at least two portions;

an authentication terminal adapted to collect a second biological individuality data and communicate with said authentication card to read said first portion of said first biological individuality data;

a certification authority adapted to communicate with said authentication terminal, wherein said certification authority includes a second portion of said first biological individuality data, and wherein said first and second portions of said first biological individuality data contain different information from within said first biological individuality data; and

an authentication device which compares said first biological individuality data from said authentication card and/or said certification authority to said second biological individuality data, wherein if said first and second biological individuality data match, authentication is verified.

21. (New) The system of claim 20, wherein said first portion of said first biological individuality data comprises less than 100% of said first biological individuality data, and wherein said second portion of said first biological individuality data comprises the remainder of said first biological individuality data.

22. (New) The system of claim 20, further comprising a policy certification authority, wherein said policy certification authority includes a third portion of said first biological individuality data, wherein said first, second and third portions do not overlap and collectively combine to comprise 100% of said first biological individuality data.

23. (New) The system of claim 22, wherein said first portion of said first biological individuality data comprises 60%, said second portion comprises 30%, and said third portion comprises 10% of said first biological individuality data.

24. (New) The system of claim 20, wherein said authentication card authenticates itself by executing a calculation at said authentication terminal.

25. (New) The system of claim 20, wherein said authentication device is adapted to apply authentication verification more than once by comparing multiple first biological individuality data with multiple second biological individuality data based on level differentiating information received from said authentication card, said authentication terminal, and/or said certification authority.

26. (New) The system of claim 20, wherein said first and second biological individuality data comprise:

fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints, wherein said authentication device selects one or more fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints to verify authentication, and wherein at least one of fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints is stored in said certification authority.

27. (New) The system of claim 26, wherein said authentication device selects said first and second biological individuality data randomly each time said authentication device compares first and second biological individuality data.

28. (New) The system of claim 20, wherein said authentication device comprises:

an authentication card reader;

an identity acquisition unit adapted to obtain said second biological individuality data;

a judgment unit adapted to collate said second biological individuality data with said first biological individuality data read from said authentication card or obtained from said certified authority; and

a display unit adapted to display a result from said judgment unit.

29. (New) A system comprising:

an authentication card including authentication data;

an authentication terminal adapted to communicate with said authentication card, wherein said authentication terminal collects comparison data;

a certification authority adapted to communicate with said authentication terminal, wherein said certification authority also includes authentication data; and

an authentication device adapted to communicate with said authentication terminal to determine a level of security and verify authentication, wherein said level of security determines a quantity of authentication and thus an amount of comparison data that must be collected and used to verify authentication, and wherein said authentication device conducts a verification of authentication based on said level of security using an effective amount of authentication data relative to said amount of comparison data collected.

30. (New) The system of claim 29, wherein said authentication data is divided between and stored in said authentication card and said certification authority.

31. (New) The system of claim 30, wherein said authentication data stored in said authentication card is less than 100% of said authentication data and wherein a remainder of said authentication data is stored in said certification authority.

32. (New) The system of claim 29, further comprising a policy certification authority including authentication data, wherein a total amount of authentication data from said authentication card, certification authority and policy certification authority is 100% of said authentication data and any authentication data in said authentication card, certification authority or policy certification authority does not overlap with any authentication data in the remaining ones of the authentication card, certification authority or policy certification authority.

33. (New) The system of claim 32, wherein said authentication card comprises 60% of said authentication data, said certification authority comprises 30% of said authentication data, and said policy certification authority comprises 10% of said authentication data.

34. (New) The system of claim 29, wherein said authentication card and said certification authority dividedly store authentication data, wherein said authentication data comprises:

fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints, wherein said authentication device selects one or more fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints, to verify authentication, wherein at least one of fingerprints, palm-prints, iris or retina patterns, DNA information, handwriting samples and/or voice prints is stored in said certification authority.

35. (New) The system of claim 29, wherein said authentication card verifies itself using a calculation executed by said authentication card at said authentication terminal.

B2

36. (New) The system of claim 20, wherein said authentication device comprises:

an authentication card reader;

an identity acquisition unit adapted to obtain said comparison data;

a judgment unit adapted to collate said comparison data with said authentication data read from said authentication card or obtained for said certified authority; and

a display unit adapted to display a result from said judgment unit.